DigiCash announces cost breakthrough in secure chip technology for smart cards

DigiCash also works together with MasterCard on EMV compliant technical testbed

FOR IMMEDIATE RELEASE (**Release Date: Tuesday, February 14, 1995**)

DigiCash bv, Amsterdam, has developed new technology allowing low-cost chips to meet the security and integrity requirements for widespread use of smart cards. "It's generally agreed that off-line transactions like credit card and stored value need public-key cryptography for security; but since public-key chips are inherently more complex and significantly more costly, most systems have been built with less secure cryptography and may need to be redone. Now we have provided a way to use public key on the least expensive and most proven chips available" said David Chaum, Managing Director of DigiCash, who revealed and demonstrated the technology for the first time at Smart Card '95 (14-16 February, 1995) in London, England. A chip, with public-key based stored value, costs under $1 U.S. It can accept multiple additional applications, at any time during the card's life, including loyalty schemes, coupons, tokens, tickets, and memberships.

In addition DigiCash has worked together with MasterCard International, N.Y.C., to develop a technical testbed integrating DigiCash's underlying technology into a card conforming to the joint Europay, MasterCard, Visa (EMV) Specification. MasterCard has been working to ensure that the EMV specification can be implemented in an unambiguous and cost effective way based on multifunctional applications, in particular the association's stored value application.

The new technology, still going by its code name "Blue" obtains its economy through a minimal requirement for silicon. It is currently implemented as firmware for the micro-controller chips produced in greatest volume: Motorola SC-24 and SGS-Thompson ST301/601, with masks for other silicon suppliers under discussion. Blue requires only 1k bytes (the smallest configuration available) of EEPROM memory, which is a main factor in the cost of chips for smart cards.

Blue also provides significant advantages in addition to public key cryptography. Most chips, for instance, can irrevocably scramble the valuable data they store when power is interrupted unexpectedly, such as could be caused by power failure or by a user removing the card too early. Blue solves this problem fully and protects all the chip's data. Other cards reveal the card identity and data content to any reader or anyone tapping communications. Blue, however, encrypts everything communicated while revealing only necessary information and only to readers with corresponding keys.

The development draws on DigiCash's 5 years of leadership in payment and chip card mask technology, and improves on the firm's innovative technology for public-key payment of highway-speed road tolls (see summary of existing products below). It is expected to be released in a form compatible with ecash, DigiCash's software- only solution to Internet payments. This would give any ecash user the option -- since only a pc connected to the Internet is required to use ecash -- of being able to obtain and carry their ecash on a smart card.

DigiCash will be supplying the technology through licensing arrangements, some of which are already in advanced stages of negotiation. Licensees can have chips produced directly by silicon suppliers and then make cards themselves, or have cards made by any of the numerous companies that put chips in cards. Inexpensive starter-kits and development packages will be supplied by DigiCash.

For more information please contact:

Paul Dinnissen
DigiCash bv
Kruislaan 419
1098 VA Amsterdam
The Netherlands
Tel: +31 20 665 2611
Fax: +31 20 668 5486
info@digicash.nl
http://www.digicash.com/

Background on related products/projects

CAFE: smart card and card-accepting electronic wallet project--Consortium founded and chaired by David Chaum of DigiCash; simulation, mask and first readers developed by DigiCash; trial this Spring at the EC headquarters building; technology trial in participation with related open special interest group, and partially funded by the EC.

DyniCash: highway-speed road-toll collection system using smart cards--Chip card inserts into battery-powered dashboard unit; reflected backscatter microwave technology by industry leader Amtech; prepaid mode has user privacy; open and/or closed pricing schemes; tested extensively in Japan; non- exclusive licensing of the payment technology.

Ecash: software only electronic cash system for internet/email--Users download software that can make and receive payments; protects users' money like travelers checks and privacy like coins; world-wide experiment with three thousand users; Macintosh, MS-Windows and X-Windows; any WWW browser; user software free with issuer licensing.

Facility Card: complete facility management smart-card/reader system--Cash replacement, access control, and time/attendance system; now in schools, hospitals, industry, offices, recreation; card store "tokens" allowing complex time, budget, and discount rules; interfaces to vending, point-of- sale, access control, copiers, phones, gaming; downloadable & upgradeable readers work on-line and/or off-line; sold through VAR's.

(Amtech, DigiCash, DyniCash, ecash (lower case "e"), Facility card, MasterCard, Motorola, and Thompson are trademarks.)

Back to the press releases page.
